CLAIMS

1. A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for:

generating a plurality of keys in response to a received challenge;

generating an initial value based upon a first key from the plurality of keys;

concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

hashing the input value to form an authentication signal; and

transmitting the authentication signal to the communications system via the communications unit.

2. The apparatus of Claim 1, wherein hashing the input value is performed in accordance with the Secure Hashing Algorithm (SHA-1).

3. The apparatus of Claim 1, wherein generating the initial value comprises padding the first key.

4. The apparatus of Claim 3, wherein generating the initial value further comprises adding the padded first key bit-wise to a constant value.

5. The apparatus of Claim 1, wherein the received signal is generated at the communications unit by:

receiving the second key from the subscriber identification module;

generating a local initial value based upon the second key;

concatenating the local initial value and a message to form a local input value;

hashing the local input value to form the received signal; and

transmitting the received signal to the subscriber identification module.

6. The apparatus of Claim 5, wherein generating the local initial value comprises padding the second key.

7. The apparatus of Claim 6, wherein generating the local initial value further comprises adding the padded second key bit-wise to a second constant value.

8. A subscriber identification module, comprising:

a key generation element; and

a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information.

9. The subscriber identification module of Claim 8, wherein the key generation element comprises:

a memory; and

a processor configured to execute a set of instructions stored in the memory, wherein the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys.

10. The subscriber identification module of Claim 9, wherein the cryptographic transformation is performed using a permanent key.

11. An apparatus for providing secure local authentication of a subscriber in a communication system, comprising a subscriber identification module configured to interact with a communications unit, wherein the subscriber identification module comprises:

a key generator for generating a plurality of keys from a received value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit; and

a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

12. The apparatus of Claim 11, wherein the subscriber identification module is configured to be inserted into the communications unit.

13. The apparatus of Claim 11, wherein the at least one communication key comprises an integrity key.

14. The apparatus of Claim 11, wherein hashing is performed in accordance with SHA-1.

15. A method for providing authentication of a subscriber using a subscriber identification device, comprising:

generating a plurality of keys;

transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys;

generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission

message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message;

transmitting the signature to the subscriber identification device;

receiving the signature at the subscriber identification device;

generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device; and

conveying the primary signature to a communications system.

16. The method of Claim 15, wherein hashing is implemented in accordance with SHA-1.

17. An apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for selectively generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station.